PRIVACY MANAGEMENT PLAN

CONTENTS

Section 1: Preliminary

1.1 INTRODUCTION

The University of Western Sydney is committed to fair personal and health information handling practices in its educational, research, engagement, and associated administrative procedures and activities.

In protecting the privacy of personal and health information entrusted to it, the University will meet its statutory requirements under the Privacy and Personal Information Protection Act (NSW) 1998 (referred to as 'PPIPA' for the rest of this document), and the Health Records and Information Privacy Act (NSW) 2002 (referred to as 'HRIPA' for the rest of this document). In particular, the University will reference its practices and activities against the Information Protection Principles ('IPPs'), and the Health Privacy Principles ('HPPs') contained in those Acts. Those principles set the standards for how the University collects, stores, uses or discloses personal and health information related to students, staff or other persons.

All staff and functional units of the University have an obligation, in their day to day practices, to adhere to and implement the privacy principles and practices established by legislation and given detailed expression in this Privacy Management Plan and other privacy related policies and guidelines.

This Privacy Management Plan applies to the University of Western Sydney and its employees. The plan aims to provide detailed information about the privacy legislation applicable to the University and about how the University deals with privacy matters. As well as being a general privacy resource, it also outlines how the University is implementing the privacy principles and reviewing its practices to ensure that it meets the provisions of the legislation.

The Privacy Management Plan was initially approved by the Vice- Chancellor and subsequent amendments and additions are approved by the University Secretary.

Any comments or queries about the Plan should be directed to the Privacy Officer (Manager, Corporate Services, Paul Woloch) via email at privacy@uws.edu.au or by telephone on 02 9678 7875.

Information about privacy at the University and access to policies and related information is available through the Privacy at the University of Western Sydney website http://www.uws.edu.au/privacy.

The University also provides a brief statement about privacy matters in its Annual Report.

1.2 PPIPA and HRIPA

The Acts that apply to the University in the main are the Privacy and Personal Information Protection Act (NSW) 1998 “PPIPA” and the Health Records and Information Protection Act (NSW) 2002 “HRIPA”. This Plan deals with each of the Acts in Sections 2 and 3 of this document.

Up until the commencement of HRIPA on 1 September 2004, PPIPA had provided for health information within its definition of personal information. HRIPA was introduced in the main to regulate the handling of health information in the public and private health sectors and although it applies to all health information its major impact is on those bodies that actually provide health services (e.g doctors, hospitals etc). At UWS the main health service provider is UniClinic within the School of Exercise and Health Sciences. For the bulk of the University (i.e. those areas that do not provide health services), the provisions and requirements of HRIPA are much the same as those already applying under PPIPA. The other area where HRIPA has a significant impact is in the area of research involving the use of health information where specific statutory guidelines are to be approved under HRIPA (Section 3 of this Plan contains detailed instructions about these issues).

1.3 COMMONWEALTH’S PRIVACY ACT, 1988

There is some confusion with respect to the existence of both State and Federal privacy legislation and while they are very similar there are some differences. To overcome these problems the Commonwealth Privacy Act 1988 includes the following section:

> s.3. It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to interferences with the privacy of persons and is capable of operating concurrently with this Act.

However, while the University is therefore subject to provisions of the NSW privacy legislation, it also remains subject to the national Privacy Act, 1988 and associated guidelines with respect to the handling of tax file numbers (TFNs). Information about these requirements can be located at:

- Privacy Act, 1988: http://www.austlii.edu.au/au/legis/eth/consol_act/pa1988108/
- Federal Privacy Commissioner: Tax file number guidelines 1992 (amended 1997) http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_53.25.pdf

The Commonwealth Act also applies to the private sector whereas the NSW Legislation (PPIPA) only applies to the public sector. HRIPA applies to both the public and private sectors. Private sector organisations that may handle personal information provided by the University (e.g. our contracted travel agents) are likely to be covered by the Commonwealth Privacy Act. However, the University needs to ensure that any information provided to another organisation is protected to the same degree that the University applies to the information it holds.

1.4 OPERATION OF THE FREEDOM OF INFORMATION ACT 1989

The operation of the Freedom of Information Act (NSW), 1989 “FOI Act” is unaffected by both PPIPA and HRIPA.

Note that FOI provides access to various documents by any person subject to the operation of various exemptions in that Act. Under PPIPA and HRIPA access to information is provided only to the person to whom the information relates.

1.5 CONFIDENTIALITY AND PRIVACY

This document addresses issues associated with privacy practices in the handling of personal and health information. In some contexts the University may have additional but related obligations of confidentiality to individuals and organisations for information received in the course of carrying out its functions. In addition, staff may have access to information that is confidential to the University but not of a personal nature (e.g. unpublished valuable research).

Confidentiality is a more general term that applies to organisations and processes as well as to individuals. Privacy confines itself to persons who have rights related to information about themselves. Organisations do not have ‘privacy’.

1.6 PRIVACY DECISIONS IN THE ADMINISTRATIVE DECISIONS TRIBUNAL

While the NSW Administrative Decisions Tribunal “ADT” is not part of the judicial system, its decisions do provide information, guidance and precedents for agencies in dealing with privacy matters.

Summaries of ADT decisions relating to privacy can be viewed at the Privacy NSW website at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index .

The Privacy Officer will periodically disseminate information about relevant ADT decisions within UWS.

1.7 STATUS OF RELATED ENTITIES

The entities are in the main subject to the Commonwealth’s Privacy Act by virtue of being ‘private sector’ incorporated bodies. The Health Records and Information Privacy Act 2002 applies to both the public and private sectors and so applies to the entities.

In any dealings between them and the University with respect to personal and health information, the standards applying to the University must be complied with.

Section 2: Privacy of Personal Information

2.1 INTRODUCTION

This section applies to all personal information other than health information.

The University of Western Sydney is committed to fair personal information handling practices that are consistent with its mission and legal obligations. The University is subject to the provisions if the NSW Privacy and Personal Information Protection Act (NSW), 1989 [PPIPA] and is required to put in place mechanisms that give effect to the principles and requirements stipulated under that Act. This covers personal information that the University collects, stores, uses, or discloses, relating to students, staff or other persons.

2.2 PERSONAL INFORMATION DEFINED

The PPIPA protects "personal information" and defines it in the following way:

> "In this Act, personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
>
> Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics." (s.4 PPIPA)

In the university context, personal information includes material like:

- Identification numbers and details (e.g. student ID)
- Contact details – addresses, telephone numbers, email addresses
- Reference numbers – tax file numbers, passport numbers, bank account numbers
- Photographic images
- Details of Next Of Kin
- Academic performance
- Health information (only until commencement of HRIPA – 1 September 2004)
- Personnel information
- Information relating to conduct
- Information or opinion about an individual arising from investigation or inquiry into matters relating to the university

Information about an individual is not considered to be personal information in certain circumstances, for example: if the person has been dead for more than 30 years; where the information is contained in a publicly available publication; or information about an individual's suitability for appointment or employment. Other exceptions relate to particular statutory responsibilities and circumstances such as information about an individual contained in a protected disclosure under the *Protected Disclosures Act, 1994*.

The University is considered to be holding personal information if:

I. It is in the possession or control of the information, or
II. the information is in the possession or control of a person employed or engaged by the University in the course of that employment or engagement, or

III. if the information is contained in a State record in respect of which the University is responsible under the *State Records Act, 1998*.

As indicated in the definition above, personal information is not just what is contained in the University's physical records (hard copy or electronic), but all personal information irrespective of format. Unlike the Commonwealth and Victorian privacy legislation, the NSW Act does not confine itself to information held in a formal record.

Under PPIPA, personal information is not collected by the University if the receipt of the information by the University is unsolicited. However, the University will in many instances receive personal information that it has not sought. For example, a prospective student making an enquiry about enrolment in a program may provide a range of personal information, some of which may be unnecessary to the application being made. While such information may be 'unsolicited' it is relevant to the functions and services of the University and as such should be treated as personal information collected by the University.

Privacy NSW, the State Government regulatory authority for privacy in NSW, provides some general guidance when considering whether in certain contexts information constitutes personal information under PPIPA.

> "It will often be necessary to look carefully at the facts and context in which information is being used to determine whether it falls within the definition of personal information or not. The following examples are based on accepted approaches to legislative interpretation although they can not be regarded as legally conclusive:
>
> - Even where personal information is held by an agency, the release of an anonymous or de-identified subset of the information is probably exempt.
>
> - An agency can collect or disclose information from a published source (eg a telephone directory) without having to follow the Act but must follow the Act for personal information from a published source which it has copied into its own records.
>
> - Information about a person's suitability for public sector employment is primarily intended to cover information used in recruitment and selection. It applies to job applications, references, service reports and pre-employment criminal record checks, but probably not to an individual's subsequent employment records.
>
> Whether information is unsolicited or not may depend on whether the agency operates a service for receiving information from the public. Even where it does receive information, gratuitous and irrelevant information may be covered by the exemption. However the agency may still need to take steps to ensure that irrelevant information is not used and reasonably comply with individuals' requests to have it deleted." (Privacy NSW, June 2003).

2.3 PERSONAL INFORMATION HELD BY THE UNIVERSITY OF WESTERN SYDNEY

As a public institution engaged in teaching, research and community service and engagement, the University holds a wide range of personal information. Broadly speaking this information relates to students, staff and members of the external community including graduates.

Students

The University collects and holds personal information related to:

- Admission information, enrolment, progression, assessment, misconduct and graduation information
- Financial information – tax file numbers, information associated with HECS
- Personal welfare (e.g. medical) information, equity group information
- Examiner's reports, fieldwork/practicum assessments

The University holds most of its student data in various management information systems, but Colleges, Schools and individual staff such as lecturers will hold and handle student personal information. The Library and Information Technology Services will also hold electronic records to identify users. UWS Security maintains records relating to car parking permits and Incident reports both of which will contain some personal information.

Staff

The University primarily holds personal information about all staff related to their employment and these files are managed by the Office of Human Resources, with significant records being held on the Concept HRMIS with some information now available via Staff Online. Some historical information related to former employees is also retained. Some staff information is also held in functional units.

The University's publications such as the calendars, the annual report and others contain some information related to staff, mainly with respect to names, position held and qualifications. The University's internal telephone directory is available via the Internet and also provides information such as name, position, telephone number, location and email address.

Externals

The University holds a range of personal information about individuals "outside" the university including graduates, benefactors and friends of the University, external members of our committees and those doing business with the University such as consultants and contractors. There is very significant contact with potential students seeking information about the University's courses via telephone, in person and via the Internet.

Some research and teaching activities involve the collection, analysis and holding of data containing personal information that may be held by the University or individual researchers. Some deposited and other records of the University may also hold personal information related to external persons.

Ethical issues associated with research, including privacy, come within the ambit of the Human Research Ethics Committee (HREC) and further information can be obtained from the Office of Research Services. In particular reference should be made to the following documents that are available via the Office of Research Services web site:

Joint NHMRC / AV-CC Statement and Guidelines on Research Practice 1997
National Statement on Ethical Conduct in Research Involving Humans 1999

Access to Personal Information Held by the University

For students, access to their official student record is via the Office of the Academic Registrar and guidance is provided in the brochure for students (Privacy and You) obtainable from Student Centres and in the document Guidelines on Disclosure and Use of Student Personal Information Access to information that may be held by specialist units such as the Library, IT Services, or the Office of the Dean of Students is obtained by direct approach to those units.

For staff, access to their personnel records is via the Office of Human Resources and a guidance document is currently under development.

For externals, access to any personal information held by the University about them should be directed to the functional unit that is understood to be holding the information.

Persons wishing to amend personal information related to them and held by the University should make that request in writing to the areas identified in the preceding paragraphs.

Where students, staff or externals have any concerns or difficulty in accessing or amending their personal information held by the University they should approach the UWS Privacy Officer for assistance.

The University will amend personal information it holds in accordance with Information Protection Principle 8, but reserves the right to make notations rather than to delete information in particular circumstances.

Nothing in this Plan or the privacy legislation affects the operation of the Freedom of Information Act, 1989 and individuals may seek access to information under that Act.

Disclosure of Personal Information Held by the University

The University provides student personal information to third parties including Commonwealth government agencies such as DEST, Centrelink, and DIMIA, to the student associations and when it is required to do so by law. Where academic programs are being offered in conjunction with another educational institution, personal information may be exchanged.

In providing personal information to other agencies, the University must ensure that:

- The disclosure is directly related to the purpose for which the information was collected and that there is no reason to believe that the individual concerned would object; or

- The individual concerned is reasonably likely to have been aware, or has been made aware that information of that kind is usually disclosed to the agency concerned; or

- There are reasonable grounds to think that disclosure is necessary to prevent or lessen a serious or imminent threat to life or health of the individual concerned or another person.

At enrolment and at other times the University indicates to students in writing that their personal information may be provided to certain other agencies and in particular circumstances.

Where the University engages a contractor or agent to undertake a function or activity on its behalf that involves the handling of personal information in some way, the University retains the legal responsibility under PPIPA for that information. Advice should be sought from UWS Legal Counsel about appropriate references in contracts and other terms of engagement.

For more detail on circumstances surrounding the disclosure of personal information relating to students (e.g. to police or in emergencies) refer to the document Guidelines on Disclosure of Student Personal Information.

Video Surveillance

The University does operate visible and open video surveillance of particular facilities such as computer laboratories and the libraries in order to protect them from damage and theft. In such instances there are prominent notices to users to advise them of the video surveillance and the cameras are not concealed. UWS Security maintains video surveillance of some University premises for security and safety reasons.

If the University were to undertake covert video surveillance, that would be done in accordance with the provisions of the Workplace Video Surveillance Act, 1998.

An Exposure Draft Workplace Surveillance Bill, 2004 was released in June 2004 for comment. This Bill deals with notified and covert surveillance by camera, computer (i.e. e-mail and internet) and by tracking a person's whereabouts. It also contains provisions restricting employers in terms of blocking e-mail or internet access.

Security of Personal Information

The security of information held by the University, including personal information, is primarily addressed in the Information Security Policy and the Records Management Policy and associated guidelines. The Privacy Policy and this Plan stipulate the requirements with respect to privacy.

2.4. INFORMATION PROTECTION PRINCIPLES

The University will comply with the information protection principles contained in PPIPA. Principles may be modified or tailored through the adoption of a privacy code of practice that is developed by an agency and/or the Privacy Commissioner and approved by the Attorney General.

The Information Protection Principles (IPPs) are as follows:

PART A – COLLECTION PRINCIPLES

IPP ONE - Collection of personal information must be for lawful purposes

The University must not collect personal information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the University, and

(b) the collection of the information is reasonably necessary for that purpose.

The University must not collect personal information by any unlawful means.

IPP TWO - Personal information must be collected directly from the individuals concerned

The University must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

(a) the individual has authorised collection of the information from someone else, or

(b) in the case of information relating to a person who is under the age of 16 years—the information has been provided by a parent or guardian of the person.

The University is not required to comply with IPP Two if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal.

IPP THREE - There is a requirement when collecting personal information to ensure that individuals are informed

If the University collects personal information from an individual, the University must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

(a) the fact that the information is being collected,

(b) the purposes for which the information is being collected,

(c) the intended recipients of the information,

(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,

(e) the existence of any right of access to, and correction of, the information,

(f) the contact details within the University of the unit collecting the information and the unit that is to hold the information.

The University is not required to comply with IPP Three if the information concerned is collected for law enforcement purposes.

IPP FOUR - Collection of personal information should have regard to relevance, necessity, accuracy and the need to be non-intrusive as far as possible

If the University collects personal information from an individual, the University must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete, and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

PART B – STORAGE PRINCIPLES

IPP FIVE - Personal information to be retained only for so long as is necessary and must be held securely

The University in holding personal information must ensure:

(a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the University, everything reasonably within the power of the University is done to prevent unauthorised use or disclosure of the information.

The University maintains its records in accordance with the provisions of the State Records Act 1998. Further information can be obtained from Records and Archive Management Services and the Records Management Policy.

PART C – ACCESS AND AMENDMENT PRINCIPLES

IPP SIX - The University must enable individuals to ascertain the nature of the information held by the University about them

The University in holding personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the University holds personal information, and

(b) whether the University holds personal information relating to that person, and

(c) if the University holds personal information relating to that person:

(i) the nature of that information, and

(ii) the main purposes for which the information is used, and

(iii) that person's entitlement to gain access to the information.

Refer to section 2.3 of this document for details about persons accessing personal information held by the University about them.

IPP SEVEN - The University must provide individuals with access to the information it holds relating to them

The University in holding personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

The provisions of the Freedom of Information Act, 1989 that impose conditions or limitations relating to access and alteration issues covered by IPPs 6, 7, and 8, continue to apply as if they were contained within PPIPA. In other words any conditions or limitations contained in the FOI Act can be used to deal with applications under IPPs 6, 7, and 8.

Refer to section 4(d) of this document for details about persons accessing personal information held by the University about them.

IPP EIGHT - The University must amend personal information to ensure it is accurate

The University in holding personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

(a) is accurate, and

(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

If the University is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the University must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the University.

Refer to section 4(d) of this document for details about persons accessing personal information held by the University about them.

PART D – USE PRINCIPLES

IPP NINE - University must check the accuracy of personal information before use

The University in holding personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

IPP TEN - The University's use of personal information is limited to the purposes for which it was collected except where the individual has agreed to the other use or in emergency circumstances

The University in holding personal information must not use the information for a purpose other than that for which it was collected unless:

(a) the individual to whom the information relates has consented to the use of the information for that other purpose, or

(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or

(c) the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

The University is not required to comply with IPP Ten if the use of the information concerned is for a purpose other than the purpose for which it was collected is reasonably necessary for law enforcement purposes or for the protection of public revenue.

PART E – DISCLOSURE PRINCIPLES

IPP ELEVEN - Disclosure of personal information is limited to the purpose for which it was collected or where the individual would be aware of the disclosure or in emergency circumstances

The University in holding personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

(a) the disclosure is directly related to the purpose for which the information was collected, and the University in disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or

(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with IPP THREE, that information of that kind is usually disclosed to that other person or body, or

(c) the University believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

If personal information is disclosed in accordance with IPP ELEVEN (1) above to a person or body that is a public sector agency such as another University, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

The University is not required to comply with IPP Eleven if the disclosure of the information concerned:

a) is made in connection with proceeding for an offence or for law enforcement purposes or,

b) is to a law enforcement agency for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

c) is authorised or required by subpoena or by search warrant or other statutory instrument, or

d) is reasonably necessary for the protection of public revenue or in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed.

In these circumstances the University is not required to disclose personal information to another person or body if the University is entitled to refuse to disclose the information in the absence of a subpoena, warrant or other lawful requirement. In these circumstances, UWS will normally only provide personal information in the context of law enforcement related to criminal investigations.

For further practical guidance on disclosure refer to the Guidelines on Disclosure of Student Personal Information.

IPP TWELVE - The University must not disclose details of an individual's beliefs, ethnic origin, health etc. except in emergency circumstances and disclosure of personal information to agencies outside New South Wales is subject to restrictions

The University must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.
The University in holding personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales unless:

(a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or

(b) the disclosure is permitted under a privacy code of practice.[1]

For the purposes of IPP TWELVE (2), a relevant privacy law means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.

The University is not required to comply with IPP Twelve if the disclosure of the information concerned is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been or may be, committed.

2.5 EXEMPTIONS RELATED TO INVESTIGATIONS UNDERTAKEN BY THE UNIVERSITY

Where the University is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency (eg Ombudsman, ICAC, etc) or that has been referred from or made by an agency to the University, then the University is:

- not required to comply with IPP Two and IPP Three if that might detrimentally affect (or prevent the proper exercise of) the University's complaint handling or investigation function
- not required to comply with IPP Ten if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in

[1] No code of practice is in operation although a draft code exists. The University's disclosures, whether interstate or elsewhere should comply with IPPs 11 and 12(1).

order to enable the University to exercise its complaint handling functions or any of its investigative functions
- not required to comply with IPP Eleven if the information concerned is disclosed to an investigative agency as defined in PPIPA (eg Ombudsman, ICAC).

2.6 PRIVACY CODES OF PRACTICE AND S.41 DIRECTIONS

Under PPIPA, Privacy Codes of Practice can be developed by agencies that provide for the modification of the application of one or more Information Protection Principles to particular activities or categories of information. This is undertaken to take account of particular circumstances relating to legitimate use of personal information by agencies that might otherwise be in contradiction to the Information Protection Principles under PPIPA.

The Privacy Commissioner can also prepare Codes of Practice common to a number of agencies. All Codes are approved by the NSW Attorney-General.

In addition, under section 41 of PPIPA the Privacy Commissioner may make a direction to waive or modify the requirement for an agency to comply with an Information Protection Principle or a Privacy Code of Practice. Mostly directions are made pending the development of a formal Code of Practice.

There are three s.41 directions that apply to the University. These are –

- Collection and disclosure for research purposes: http://www.lawlink.nsw.gov.au/pc.nsf/pages/s41research

While the full text of this direction should be viewed it basically provides certain exemptions from the requirements of the Act to an agency for:

a. Research where an ethical research committee exists and has considered the privacy issues and approved the research;
b. Personal information contained in records deposited with an agency for purposes that include research; and
c. Personal information collected and used to provide reference material to collections of historical or cultural significance.

- The Use of Information for Investigative Purposes: http://www.lawlink.nsw.gov.au/pc.nsf/pages/s41invest

While the full text of this direction should be viewed it basically provides certain exemptions from the requirements of the Act to an agency where non-compliance is reasonably necessary for the proper exercise of any of the agency's investigative functions or its conduct of any lawful investigations.

- Some information transfers between public sector agencies: http://www.lawlink.nsw.gov.au/pc.nsf/pages/s41interag

While the full text of this direction should be viewed it basically provides certain exemptions from the requirements of the Act relating to where exchanges of information between agencies are reasonably necessary for the purpose of dealing with:

a. Responses to correspondence from Ministers or MPs;
b. Referral of inquiries;
c. Auditing accounts or performance of a program or programs administered by an agency or agencies;
d. Law enforcement purposes not covered by the exemptions in the Act;
e. Performance agreements between agencies.

2.7 PUBLIC REGISTERS

Under PPIPA a Public Register is defined as being "a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)."

The University does not have any Public Registers although it makes a range of information available via its publications. Academic staff for example are listed in the annual Calendars.

The University maintains records of all its graduates. After students graduate the University makes certain information available to those with a legitimate interest in confirming that information, such as employers or other academic institutions. The information made available on an open basis is:

- Name of graduate
- Name of award conferred
- Date of conferral

Section 3: Privacy of Health Information

3.1. INTRODUCTION

This section applies to health information and also to a limited extent to personal information but only where that has been collected in the context of providing a health service.

The University of Western Sydney is committed to fair personal and health information handling practices that are consistent with its mission and legal obligations.

The University is subject to the provisions of the NSW Health Records and Information Privacy Act, 2002 (HRIPA) and is required to put in place mechanisms that give effect to the principles and requirements stipulated under that Act. This covers personal and health information that the University collects, stores, uses, or discloses, relating to students, staff or other persons. The provisions of HRIPA commence on 1 September 2004.

The purpose of HRIPA as applied to the University is basically to: protect the privacy of an individual's health information that is held by the University; enable individuals to gain access to that information and; to provide a framework for the resolution of complaints regarding the handling of health information.

3.2 PERSONAL INFORMATION AND HEALTH INFORMATION DEFINED

The Health Records and Information Privacy Act 2002 (HRIPA), defines "personal information" in the following way:

> In this Act, personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
>
> Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

This definition of personal information is identical to that found in the Privacy and Personal Information Protection Act 1998 (PPIPA) along with the specified exemptions.

The Health Records and Information Privacy Act 2002 (HRIPA), protects "health information" and defines it in the following way:

> Health information means:
>
> (a) personal information that is information or an opinion about:
> (i) the physical or mental health or a disability (at any time) of an individual, or
> (ii) an individual's express wishes about the future provision of health services to him or her, or
> (iii) a health service provided, or to be provided, to an individual, or
> (b) other personal information collected to provide, or in providing, a health service, or

(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or
(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual,

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

3.3 HEALTH PRIVACY POLICY STATEMENT

The University of Western Sydney is committed to fair health information handling practices in its educational, research, engagement, and associated administrative procedures and activities in order to protect the privacy of individuals.

In protecting the privacy of health information entrusted to it, the University will meet its statutory requirements under the Health Records and Information Privacy Act 2002 (HRIPA) and other relevant legislation. In particular the University will reference its practices and activities against the Health Privacy Principles (HPPs) contained in that Act.

All staff and functional units of the University have an obligation, in their day-to-day practices, to adhere to and implement the Health Privacy Principles and practices established by legislation and given detailed expression in this and other privacy related policies and guidelines.

3.4. APPLICATION TO THE UNIVERSITY OF WESTERN SYDNEY

The University is subject to the provisions of HRIPA both as a provider of certain health services and as a public sector agency generally. The University also has a major function with respect to the education and training of health care professionals (particularly nurses) and is engaged in health related research. Areas and activities of the University that would handle health information in some form or manner are as follows.

As a health service provider:

- case records of Uniclinic within the School of Exercise and Health Science
- case records of the clinics within the School of Psychology
- case records of the University's student counselling service

As a public educational institution:

- research involving the use of health information
- education and training of students, including requirements related to clinical practice undertaken by students with other organisations
- health information of students related to their enrolment and progress through their academic program (e.g. deferred examinations, special consideration, disability etc.)

As an employer:

- health information of staff related to their employment (e.g. medical reports, sick leave certificates, disability information, etc.)
- Workers Compensation and Occupational Health and Safety files.

The University is considered to be holding health information if:

i. it is in possession or control of the information, or
ii. the information is in the possession or control of a person employed or engaged by the University in the course of that employment or engagement, or
iii. if the information is contained in a State record in respect of which the University is responsible under the *State Records Act 1998*.

Health information is not collected by the University if the receipt of the information by it is unsolicited.

3.5 HEALTH PRIVACY PRINCIPLES (HPPS)

The University will comply with the health privacy principles contained in HRIPA (Schedule 1). The principles may be modified or tailored through the adoption of a health privacy code of practice that is developed by the University and/or the Privacy Commissioner and approved by the Attorney General.

The Health Privacy Principles (HPPs), in summary form, are as follows. The full text of the HPPs is contained in Appendix A.

PART A – COLLECTION PRINCIPLES

HPP ONE - Collection of health information must be for lawful and necessary purposes

The University must only collect health information for a lawful purpose that is directly related to a function or activity of the University, and where the information is reasonably necessary for that purpose.

HPP TWO – The health information must be relevant, not excessive, accurate and not intrusive

The University must take reasonable steps to ensure that the health information it collects is relevant to the purpose, is not excessive, and is accurate, up to date and complete. Also the collection of the health information must not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

HPP THREE - Health information must be collected directly from the individual/s concerned

The University must collect health information about an individual only from that individual, unless it is unreasonable or impractical to do so.

HPP FOUR - There is a requirement when collecting health information to ensure that individuals are informed of certain matters

When the University collects health information about an individual from the individual, it must take reasonable steps to ensure that the individual (or in the case of incapacity, the individual's authorised representative) is aware of:

- how to contact the University and request access to the information;
- the purpose for which the information is collected;
- if the information is likely to be disclosed to others;
- any legal requirements on the University to collect the information;
- any consequences for the individual if the information is not provided.

Where the University collects health information about an individual from someone else, it must take reasonable steps to ensure that the individual is generally aware of the matters listed above except where making the individual aware of the matters would pose a serious threat to the life or health of any individual.

The University may not be required to comply with the requirements of this Principle in certain particular circumstances such as legal compliance or law enforcement. These exemptions are spelt out in detail in Appendix A (clause 4).

PART B – STORAGE PRINCIPLES

HPP FIVE - Health information to be retained only for so long as is necessary and must be held securely

The University must ensure that health information is held securely and for no longer than is necessary. It must also ensure that health information is protected by taking reasonable security safeguards against: loss; unauthorised access, use, modification or disclosure; and against any other misuse.

The University is required to maintain its records in accordance with the provisions of the State Records Act 1998. Further information can be obtained from Records and Archive Management Services and the Records Management Policy.

PART C – ACCESS AND AMENDMENT PRINCIPLES

HPP SIX - The University must enable individuals to ascertain the nature of the health information held by the University about them

The University must enable any person to ascertain whether it holds health information about them and the nature and purpose of that information. It must also advise them that they can gain access to it.

HPP SEVEN - The University must provide individuals with access to the health information it holds relating to them

Where the University holds health information about an individual it must, when requested by the individual, provide the individual with access to the information.

Note that access to and amendment of health information may also be able to be sought under the Freedom of Information Act 1989.

HPP EIGHT - The University must amend/annotate health information to ensure it is accurate

Where the University holds health information about an individual it must, when requested by the individual, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information is accurate and, having regard to the purpose for which it is to be used, is relevant, up to date, complete and not misleading.

If the University and the individual disagree about the making of any amendments the University must, if requested by the individual, attach to the information a statement provided by that individual of the amendment sought.

Where health information is amended under this Principle, the individual is entitled, if reasonably practicable, to have recipients of that information notified of the amendments made by the University.

PART D – USE PRINCIPLES

HPP NINE - University must check the accuracy of health information before use

The University must not use health information without taking reasonable steps to ensure that the information is relevant, accurate, up to date, complete and not misleading, having regard to the purpose for which it is to be used.

HPP TEN - Use of health information is limited to the purposes for which it was collected except where the individual has consented to the other use or in other defined circumstances

The University must only use[2] health information for the purpose for which it was collected, and not for another or secondary purpose, unless:

- the individual has specifically consented[3] to the other use;
- the other purpose is directly related and the individual would reasonably expect the University to use the information in that way;
- there is a serious and imminent threat to the health, safety or welfare of the individual or another person or to public health or safety.

The University may use health information for the secondary purposes of the management of health services (i.e. in relation to the provision of a health service), the

[2] Note that the principles surrounding use and disclosure apply within the University in the sense that health information provided to one section of the University for a particular purpose may not be used by or disclosed to another section of the University other than in accordance with these Health Privacy Principles.

[3] With respect to consent it is important that the individual provides informed consent (i.e. has the capacity to understand) and is providing it on a voluntary basis. Consent should be obtained in writing wherever possible and should be specific to the circumstances and be current. While it is acceptable to obtain verbal consent or to rely on implied consent if it is not practicable to obtain written consent, that may be problematic if a dispute arises in the future. General cover-all consents should be avoided.

provision of training, or the undertaking of research. This use is subject to the conditions that:

- the purpose cannot be achieved through the use of de-identified data;
- it is impractical to seek consent to the use from the individual/s;
- the information is de-identified as far as possible;
- the information is not published in a generally available publication where it is in a form that would enable individuals to be identified; and
- any guidelines issued by the Privacy Commissioner are complied with.

The University may also use health information in a range of specified contexts as outlined in detail in the Appendix (clause 10). These include circumstances related to: the finding of missing persons; unlawful activity or misconduct or investigations within the University; and law enforcement or investigative functions of investigative agencies (e.g. ICAC).

PART E – DISCLOSURE PRINCIPLES

HPP ELEVEN - Disclosure of health information is limited to the purpose for which it was collected except where the individual has consented to the other disclosure or in other defined circumstances

The University must only disclose health information for the purpose for which it was collected, and not for another or secondary purpose, unless:

- the individual has specifically consented to the other disclosure;
- the other purpose is directly related and the individual would reasonably expect the University to disclose the information in that way;
- there is a serious and imminent threat to the health, safety or welfare of the individual or another person or to public health or safety.

The University may disclose health information for the secondary purposes of the management of health services (i.e. in relation to the provision of a health service), the provision of training, or the undertaking of research. This disclosure is subject to the conditions that:

- the purpose cannot be achieved through the disclosure of de-identified data;
- it is impractical to seek consent to the disclosure from the individual/s;
- the information is de-identified as far as possible;
- the information is not published in a generally available publication where it is in a form that would enable individuals to be identified; and
- any guidelines issued by the Privacy Commissioner are complied with.

The University may also disclose health information in a range of specified contexts as outlined in detail in the Appendix (clause 11). These include circumstances related to: disclosure to an immediate family member for compassionate reasons; the finding of missing persons; unlawful activity or misconduct or investigations within the University; and law enforcement or investigative functions of investigative agencies (e.g. ICAC).

PART F – USE OF IDENTIFIERS PRINCIPLES

HPP TWELVE – Identifiers only to be used where necessary

An identifier is usually a number that is assigned to an individual in conjunction with that individual's health information for the purpose of uniquely identifying them. The University may only assign identifiers to individuals if that is reasonably necessary to enable the University to carry out any of its functions related to the handling of health information efficiently.

PART G – ANONYMITY PRINCIPLES

HPP THIRTEEN – Individuals to have the opportunity of anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from the University.

PART H –TRANSFER OUT OF NSW PRINCIPLES

HPP FOURTEEN – Health information not to be transferred out of New South Wales except under specified conditions

The University may only transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency where:

- the recipient of the information is subject to health privacy provisions similar to those in NSW; or
- the individual has consented; or
- the transfer is part of an agreed contract in the interests of the individual; or
- the transfer benefits the individual, and it is impractical to obtain consent, and the individual would be likely to agree; or
- the transfer will lessen or prevent a serious and imminent threat to the health, safety or welfare of the individual or another person or to public health or safety; or
- steps have been taken to ensure that the information will not be used or disclosed contrary to the Health Privacy principles; or
- the transfer is permitted or required by law.

PART I –LINKAGE OF HEALTH RECORDS PRINCIPLES

HPP FIFTEEN – Linkage of health records generally not to occur without express consent

The University may only include health information about an individual in a health records linkage system, or disclose an identifier for the same purpose, where the individual has given their consent or where:

- it is legally required or authorised to do so; or
- it is undertaken for research purposes in accordance with the provisions relating to research under HPPs 10 and 11.

In this HPP:

health record means an ongoing record of health care for an individual;
health records linkage system means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

3.6 HEALTH PRIVACY CODES OF PRACTICE AND STATUTORY GUIDELINES

The Privacy Commissioner, the University or any other organisation may develop health privacy codes of practice. The purpose of such codes is to regulate the handling of health information and they may modify the application of any of the Health Privacy Principles to any organisation or class of organisations. Codes of practice are subject to approval by the Minister for Health.

In addition, exemptions from the Health Privacy Principles (HPPs) may be subject to the operation of statutory guidelines that outline in detail how an exemption is to be applied. It is important to recognise that where the exemptions are being invoked by the University in any of its activities it is mandatory that any Guidelines be complied with.

As at July 2004 four statutory guidelines have been developed and are awaiting Ministerial approval. The draft guidelines are:

(a) Statutory guidelines on the management of health services (HPP 10 and 11)
(b) Statutory guidelines on training. (HPP 10 and 11)
(c) Statutory guidelines on research (HPP 10 and 11)
(d) Statutory guidelines on notifying a person when you have collected health information about them from someone (HPP 4)

When approved these guidelines will be summarised in this Guide. In the interim the discussion drafts can be accessed via the Privacy NSW web site at:
http://www.lawlink.nsw.gov.au/pc.nsf/pages/hripaguidelines

3.7 HEALTH PRIVACY COMPLAINTS AND INTERNAL REVIEW PROCEDURES

Under HRIPA the complaints procedure to be applied where a person believes that the University may have breached a Health Privacy Principle (HPP) or a health privacy code of practice that applies to the University is that provided for under the Privacy and Personal Information Protection Act 1998.

Details of the complaint and internal review procedure that will be used are contained in Section 4 of this document.

Uniclinic in the School of Exercise and Health Sciences is a direct provider of health services and maintains patient files. As such it has its own procedures for handling privacy related complaints.

Section 4: Privacy Related Complaints and Internal Review Procedures

4.1 INTRODUCTION

Where a person has a privacy complaint that relates to the way in which the University has managed the person's personal or health information then the University may need to deal with the matter as an Internal Review.

Internal Review procedures will apply where it is alleged that the University:

(a) has breached a privacy protection or health privacy principle or
(b) has breached a privacy code of practice applying to the University or
(c) has breached the public register provisions of the Act.

If a matter does not fall into these categories then it should be dealt with as a regular complaint. If it is unclear whether the matter should be an Internal Review or not it should be referred to the Privacy Officer for advice.

4.2 INTERNAL REVIEW APPLICATIONS

An Internal Review application must be in writing and should be lodged within six months from the time the complainant first became aware of the conduct that is the subject of the application. An application form is available: Privacy Complaints: Internal Review Application Form. Applications are to be forwarded to the University Secretary.

4.3 HOW IS THE INTERNAL REVIEW CONDUCTED?

On receipt of the application the University Secretary will determine who will conduct the review. The person must be an employee of the University but may seek legal or other assistance. They must not have been involved in a substantive way in matters that are the subject of the application. A guideline is available to staff on the process for undertaking an Internal Review.

In accordance with the requirements of PPIPA the University must notify the Privacy Commissioner of the Review applications it receives, the progress made in dealing with applications, and the findings and any actions taken. The Privacy Commissioner is entitled to make submissions to the University with respect to applications and may at the request of the University undertake the Review on behalf of the University. In conducting an Internal Review the University will follow the procedures recommended by Privacy NSW.

The review must be completed by the University within 60 days of the lodgement of the application. The University has 14 days in which to advise the applicant of the outcome.

Once a review has been completed, the University may decide to:

i. take no further action
ii. make a formal apology
iii. take appropriate remedial action, which could include payment of compensation
iv. give an undertaking that the conduct will not recur
v. implement measures to prevent recurrence of the conduct

4.4 NOTIFICATION TO THE COMPLAINANT

When notifying the applicant of the outcome of the complaint, the following information will be provided:

i. findings of the Review
ii. the reasons for the finding
iii. the action proposed to be taken
iv. the reasons for the proposed action
v. the applicant's right to a review of the finding by the Administrative Decisions Tribunal

If a person is not satisfied with the outcome of a Review or if the University has not dealt with the matter within 60 days, then the person may seek a review of the conduct complained about by the Administrative Decisions Tribunal. The Tribunal has a wide power under section 55 of the Act to make orders including the awarding of damages up to $40,000.

The person, if not satisfied with the outcome of the Administrative Decisions Tribunal has a right of appeal to the Appeal Panel of the Tribunal.

4.5 ASSISTANCE WITH COMPLAINTS

Advice and assistance with applications can be accessed via the UWS Privacy Officer. The University will provide information in hardcopy and on the web to inform potential complainants of their right to seek an Internal Review, how to lodge an application, the role of the Privacy Commissioner in the review process, the outcomes that might be expected and the rights of appeal.

Section 5: References, Further Information and Contacts

University Policies and Documents

The University has developed a range of statements and policies related to privacy, as follows:

- Privacy Policy
- Guidelines on Disclosure and Use of Student Personal Information
- Privacy Management Plan
- *Privacy and You* brochure for students
- *Information about Health Privacy for UWS Students Undertaking Clinical Experience (or other placement) in the Health Sector* brochure for students
- Guidelines on Disclosure and Use of Staff Personal Information (under development)
- Records Management Policy
- Information Security Policy

These documents are accessible via the University's Privacy web site:
http://www.uws.edu.au/privacy

UWS Contact Points

Privacy matters are the responsibility of all functional units within the University. Initial inquiries about information held should be directed to the unit that holds the information. In particular advice about student and staff records and personal information should be directed to:

For students: Academic Registrar or nominee
For staff: Director Human Resources or nominee

With respect to the specific health related services provided by the University and associated health records, contact should be made direct with the Units as follows:

Uniclinic within the School of Exercise and Health Science – Clinic Manager
Clinics within the School of Psychology – Clinic Secretary
The University's student counselling service – Head Counselling and Disabilities Services

Overall privacy management, general advice and applications for review are managed by the Division of Corporate Services. Privacy matters and issues can be accessed via the UWS website at: http://www.uws.edu.au/privacy

Inquiries should be directed to:

The Privacy Officer
Division of Corporate Services
Email: privacy@uws.edu.au

External Contact Points

Contact details for the Privacy NSW and the associated website that includes useful explanatory information about rights with respect to privacy, explanations of the legislation, and other links are as follows:

Privacy NSW
Level 17, 201 Elizabeth Street
Sydney 2000

PO Box A2122
Sydney South NSW A1235

Telephone: 02 9268 5588
Web Site:
http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index

NSW Legislation

The Health Records and Information Privacy Act 2002 and the Privacy and Personal Information Protection Act, 1998 (PPIPA) can be accessed via the NSW Parliamentary Counsel's Office website: http://www.legislation.nsw.gov.au

Training for Staff

Formal training programs are offered twice yearly. For information contact the Privacy Officer at privacy@uws.edu.au.

An online training program is loaded onto the UWS Privacy Website and available to staff to work through. The program deals with the Privacy and Personal Information Protection Act 1998 (PPIPA).

Section 6: Privacy Implementation Strategies Schedules

PRIVACY STRATEGIES IMPLEMENTATION AT UWS

Through the operation of this Plan the University aims to review and improve its practices on an ongoing basis with respect to privacy management across the University. Maintaining compliance with the Personal Information Protection Principles and Health Privacy Principles is a responsibility for all staff in their day-to-day activities. This Part identifies particular areas of the University's administration that regularly handle personal information with a view to developing strategies and review processes to ensure that the University meets its privacy obligations.

APPENDIX A - PRIVACY (PPIPA) IMPLEMENTATION STRATEGY SCHEDULE

Functional Area:	**Development & International Division**				
Issue for Consideration	**Proposed Strategy**	**Responsibility**	**Outcome/Comments**	**Completion/Review Date**	**Action**
Determination of the status of the UWS related entities with respect to privacy legislation at State and Federal level.	Consultation with entities, provision of legal advice, provision of advise to University and entities.	Director OBD, UWS Legal Counsel, Privacy Officer	Clearer understanding of statutory responsibilities with respect to privacy.	End 2003. **Extended to End 2004.** Ongoing.	Certain entities are subject to legislation under either State or Federal Law.
Compliance in research practices.	Conduct review of practices with respect to privacy and research data and oversight of that via Human Ethics Committee. Assessment of level of compliance with Personal Information Protection Principles and the Section 41 directions on research.	Directors ORS	Clearer understanding of statutory responsibilities with respect to privacy and application in the research context.	**Extended to August 2004.**	COMPLETED ORS have completed revised guidelines and are awaiting approval.
Video Surveillance and Security practices.	Review requirements with respect to video surveillance. Examine practices of UWS and initiate any needed changes. Examine any issues associated with videoconferencing.	Director Capital Works, Director IT, Director Educational Development	Certification that practices meet privacy requirements.	End March 2004. **Extended to End 2004.**	KC to organise meeting with Brian Castelli & PW to discuss. Schedule for Sept/Oct. *NOTE: New legislation in effect regarding surveillance.*
Access to personal information by security staff.	Review requirements with respect to video surveillance. Examine practices of UWS and initiate any needed changes.	Director Capital Works & Facilities. Director IT. Director Educational Development.	Certification that practices meet privacy requirements.	End March 2004. **Extended to End 2004.**	KC to organise meeting with Brian Castelli & PW to discuss. Schedule for Sept/Oct. *NOTE: New legislation in effect regarding*

	Examine any issues associated with videoconferencing.				*surveillance.*
International student's information.	Review privacy requirements against ESOS compliance requirements.	Director International Compliance Officer.	Certification that practices meet privacy requirements.	Certification that meet privacy requirements.	KC to Contact Geza Karacsony – check about ESOS reporting requirements & legal compliance issues. Consider disclaimer on Website, publishing of information.
Functional Area:	**Corporate Services Division**				
Issue for Consideration	**Proposed Strategy**	**Responsibility**	**Outcome/Comments**	**Completion/Review Date**	**Action**
Record Keeping	Review records management policy and procedures to ensure that privacy requirements are met.	Manager RAMs unit.	**COMPLETED** Refer Michael Smith.	**End December 2003.** Ongoing.	COMPLETED GDA 9 in effect.
Marketing activities and external contacts.	Review OMC procedures and practices with respect to: Handling of incoming requests for information (via web & telephone). Alumni contacts & records. Development consultants & records. Use of students in media campaigns, publications	Director OMC. Privacy Officer.	Adherence to policy and legislation.	**End June 2004.**	COMPLETED OMC have own Privacy Management Plan in effect. KC to contact Debbie Young to request copy of PMP.

	etc. Marketing surveys.				
Human Resource practices.	Produce statement about access to staff records, and privacy & confidentiality procedures relating to the process of releasing information about staff.	Director HR.	Clear understanding by HR staff of procedures for management of employee records.	End June 2004. **Extended to End 2004.**	KC to contact Narelle Kennedy to organise meeting with PW.
Review of statistical and management information data from a privacy perspective.	Review nature and use of data in EIS being developed to assess degree of use of personal information. Develop guidelines on collection, use & storage of such information in the EIS. Incorporate NSW Government (OIT) Information Security Guidelines into planning of development processes.	Director Planning & Quality.	Security of personal information contained in EIS.	End March 2004. **Extended to End 2004.**	KC to organise meeting with Stephen Butler and PW. Schedule for Oct/Nov.
Privacy Agreements with third parties.	Review need and develop generic agreement clauses related to protection of confidentiality & privacy where third parties are given access to university information.	UWS Office of Legal Counsel.	Need to ensure that where contractors and other handle university information that there is adequate protection in place.	End March 2004.	KC to contact Tanya Davies/ Andrea (legal) regarding UWS Contracts. ➢ Consider: ➢ Contractors ➢ IT department ➢ Mail houses
Implications for UWS of HRIP Act 2002 (WEF 1 Sept 2004)	Establish Reference Group – CSHS. Review legislation and provide responses and input to draft guidelines	Assoc Dean CSHS. Privacy Officer. Director ORS.	Understanding and compliance with new legislation.	End March 2004. **GROUP ESTABLISHED** INITIAL HRIPA ISSUES IDENTIFIED	COMPLETED PW has organised training for CSHS staff at Campbelltown

	by Privacy NSW & NSW Health. Develop guidelines and information for promulgation within relevant areas of UWS related to both staff and students.	Director HR. Academic Registrar (or nominee).		ONGOING IMPLEMENTATION AND MANAGEMENT	Campus (15 Sept) provided by Privacy NSW.
Ongoing privacy management and dissemination of information and training.	Establish privacy reference group representative of key areas for dissemination of privacy related information, review of privacy compliance progress under the PMP. Such officers to be responsible for the follow up related to actions under this plan.	Privacy Officer/Privacy Co-Ordinator.	Adequate knowledge and information about privacy.	End 2004. **GROUP ESTABLISHED** Ongoing review & dissemination of information as required.	The group has been asked to invite staff from their area to attend training session in September regarding Privacy at UWS. KC to organise meeting with group at EOY to consider privacy priorities for each area.
As Above	Plan periodical general and specialist training programs related to privacy and incorporation of privacy issues in to other relevant programs. Ongoing professional development for staff in key roles with primary responsibilities.	Privacy Officer. Manager PDU. Director HR.	Adequate knowledge and information about privacy.	End June 2004. **GROUP ESTABLISHED** Ongoing review & dissemination of information as required.	
As Above	Establish privacy website for dissemination of information and also disseminate information via email and staff newsletter.	Privacy Officer.	Adequate knowledge and information about privacy.	End March 2004. **WEBSITE ESTABLISHED** Ongoing updating and modification as required.	KC to post new and updated information on Privacy website.
As Above	Implement on-line privacy training module developed by Privacy NSW and Dept of	Privacy Officer.	Adequate knowledge and information about privacy.	End 2003. **ON-LINE TRAINING UP ON WEB**	Kristin to complete training module.

	Commerce for NSW Govt agencies.			Ongoing review.	
As Above	Establish database/spreadsheet for recording issues, complaints and advice given related to privacy.	Privacy Officer.	Adequate knowledge and training about processes. Complaints officer appointed for UWS.	End June 2004. **Extended to End 2004.** Ongoing implementation and review.	KC to develop SS/DB for recording privacy queries and answers as they arise for future reference/posting on website.
As Above	Develop protocol for handling privacy enquiries and complaints.	UWS Complaints Officer. Privacy Officer. UWS Legal Counsel.	Adequate knowledge of complaints process and further external sources to refer to if required. Effective complaints handling.	End June 2004. **Extended to End 2004.** Complaints process being developed. Ongoing review.	Complaints process in development (Linda Watson – Complaints Officer). Privacy complaints will be integrated in to this process.
Functional Area:	**Academic Services Division**				
Issue for Consideration	**Proposed Strategy**	**Responsibility**	**Outcome/Comments**	**Completion/Review Date**	**Action**
Privacy considerations in teaching and learning.	Conduct review of privacy practices in teaching and learning context including: WebCT and on-line learning protocols and moderation/surveillance. Teacher/student privacy and confidentiality of information practices relating to potential dissemination or release of student personal information by lecturers. Student evaluations of teaching and units. Develop training and	Director Educational Development. Academic Registrar (or nominee). PVC Academic (or nominee). Assoc Deans of Colleges.	Clear guidelines for academic staff and students about privacy issues and practices relevant to their day to day academic work and interactions.	End June 2004. **Extended to End 2004.** Ongoing.	Consider some common issues to be posted on to Privacy website.

	information material for academic staff and students.				
Privacy considerations in personal information about students held by the Office of the Dean of Students.	Review practices in area of student counselling, student scholarships, Golden Key etc.	Dean of Students.	Certification that practices adhere to privacy requirements.	End March 2004. **Extended to End 2004.**	
Privacy Considerations in IT systems.	Review of ITS policies and procedures regarding privacy. Ensure all video surveillance activity is properly signposted and that there are proper procedures associated with the storage and use of surveillance tapes. Ensure Information Security Policy and practices protect personal data. Consider issue of mobile telephones with cameras.	Director ITS for all. Director Capital Works & Facilities. Security.	Certification that systems meet privacy requirements.	End June 2004. **Extended to End 2004.**	Email policy developed and awaiting approval. PW to review. Schedule for Oct/Nov.
Review of privacy in student administrative systems.	Review Callista system and protocols with respect to privacy requirements. Review student administration forms to ensure proper advise to students about privacy at UWS. Develop plain English brochure for students about privacy. Develop comprehensive	Academic Registrar (or nominee). Privacy Officer.	Certification that practices adhere to privacy requirements.	End September 2004. **Extended to End 2004.**	Callista review completed. Student forms review ongoing. Plain English brochure ongoing. Statement on release of student info ongoing. Training for staff organised and running.

	statement about procedures and requirements surrounding release of information about students. Develop training for ‘front line’ staff to ensure they have confidence in dealing with privacy.				

APPENDIX B - HEALTH PRIVACY (HRIPA) IMPLEMENTATION STRATEGY SCHEDULE

Functional Area:	**Development & International Division**				
Issue for Consideration	**Proposed Strategy**	**Responsibility**	**Outcome/Comments**	**Completion/Review Date**	**Action**
Determination of the status of the UWS related entities with respect to privacy legislation at State and Federal level.	Consultation with entities, provision of legal advice, provision of advise to University and entities.	Director OBD, UWS Legal Counsel, Privacy Officer	Clearer understanding of statutory responsibilities with respect to privacy.	End 2003. **Extended to End 2004.** Ongoing.	Certain entities are subject to legislation under either State or Federal Law.
Compliance in research practices.	Conduct review of practices with respect to privacy and research data and oversight of that via Human Ethics Committee. Assessment of level of compliance with Personal Information Protection Principles and the Section 41 directions on research.	Directors ORS	Clearer understanding of statutory responsibilities with respect to privacy and application in the research context.	**Extended to August 2004.**	COMPLETED ORS have completed revised guidelines and are awaiting approval.
Video Surveillance and Security practices.	Review requirements with respect to video surveillance. Examine practices of UWS and initiate any needed changes. Examine any issues associated with videoconferencing.	Director Capital Works, Director IT, Director Educational Development	Certification that practices meet privacy requirements.	End March 2004. **Extended to End 2004.**	KC to organise meeting with Brian Castelli & PW to discuss. Schedule for Sept/Oct. *NOTE: New legislation in effect regarding surveillance.*
Access to personal information by security staff.	Review requirements with respect to video surveillance. Examine practices of UWS and initiate any needed changes.	Director Capital Works & Facilities. Director IT. Director Educational Development.	Certification that practices meet privacy requirements.	End March 2004. **Extended to End 2004.**	KC to organise meeting with Brian Castelli & PW to discuss. Schedule for Sept/Oct. *NOTE: New legislation in effect regarding*

	Examine any issues associated with videoconferencing.				*surveillance.*
International student's information.	Review privacy requirements against ESOS compliance requirements.	Director International Compliance Officer.	Certification that practices meet privacy requirements.	Certification that meet privacy requirements.	KC to Contact Geza Karacsony – check about ESOS reporting requirements & legal compliance issues. Consider disclaimer on Website, publishing of information.
Functional Area:	**Corporate Services Division**				
Issue for Consideration	**Proposed Strategy**	**Responsibility**	**Outcome/Comments**	**Completion/Review Date**	**Action**
Record Keeping	Review records management policy and procedures to ensure that privacy requirements are met.	Manager RAMs unit.	**COMPLETED** Refer Michael Smith.	**End December 2003.** Ongoing.	COMPLETED GDA 9 in effect.
Marketing activities and external contacts.	Review OMC procedures and practices with respect to: Handling of incoming requests for information (via web & telephone). Alumni contacts & records. Development consultants & records. Use of students in media campaigns, publications	Director OMC. Privacy Officer.	Adherence to policy and legislation.	**End June 2004.**	COMPLETED OMC have own Privacy Management Plan in effect. KC to contact Debbie Young to request copy of PMP.

	etc. Marketing surveys.				
Human Resource practices.	Produce statement about access to staff records, and privacy & confidentiality procedures relating to the process of releasing information about staff.	Director HR.	Clear understanding by HR staff of procedures for management of employee records.	End June 2004. **Extended to End 2004.**	KC to contact Narelle Kennedy to organise meeting with PW.
Review of statistical and management information data from a privacy perspective.	Review nature and use of data in EIS being developed to assess degree of use of personal information. Develop guidelines on collection, use & storage of such information in the EIS. Incorporate NSW Government (OIT) Information Security Guidelines into planning of development processes.	Director Planning & Quality.	Security of personal information contained in EIS.	End March 2004. **Extended to End 2004.**	KC to organise meeting with Stephen Butler and PW. Schedule for Oct/Nov.
Privacy Agreements with third parties.	Review need and develop generic agreement clauses related to protection of confidentiality & privacy where third parties are given access to university information.	UWS Office of Legal Counsel.	Need to ensure that where contractors and other handle university information that there is adequate protection in place.	End March 2004.	KC to contact Tanya Davies/ Andrea (legal) regarding UWS Contracts. ➢ Consider: ➢ Contractors ➢ IT department ➢ Mail houses
Implications for UWS of HRIP Act 2002 (WEF 1 Sept 2004)	Establish Reference Group – CSHS. Review legislation and provide responses and input to draft guidelines	Assoc Dean CSHS. Privacy Officer. Director ORS.	Understanding and compliance with new legislation.	End March 2004. **GROUP ESTABLISHED** INITIAL HRIPA ISSUES IDENTIFIED	COMPLETED PW has organised training for CSHS staff at Campbelltown

	by Privacy NSW & NSW Health. Develop guidelines and information for promulgation within relevant areas of UWS related to both staff and students.	Director HR. Academic Registrar (or nominee).		ONGOING IMPLEMENTATION AND MANAGEMENT	Campus (15 Sept) provided by Privacy NSW.
Ongoing privacy management and dissemination of information and training.	Establish privacy reference group representative of key areas for dissemination of privacy related information, review of privacy compliance progress under the PMP. Such officers to be responsible for the follow up related to actions under this plan.	Privacy Officer/Privacy Co-Ordinator.	Adequate knowledge and information about privacy.	End 2004. **GROUP ESTABLISHED** Ongoing review & dissemination of information as required.	The group has been asked to invite staff from their area to attend training session in September regarding Privacy at UWS. KC to organise meeting with group at EOY to consider privacy priorities for each area.
As Above	Plan periodical general and specialist training programs related to privacy and incorporation of privacy issues in to other relevant programs. Ongoing professional development for staff in key roles with primary responsibilities.	Privacy Officer. Manager PDU. Director HR.	Adequate knowledge and information about privacy.	End June 2004. **GROUP ESTABLISHED** Ongoing review & dissemination of information as required.	
As Above	Establish privacy website for dissemination of information and also disseminate information via email and staff newsletter.	Privacy Officer.	Adequate knowledge and information about privacy.	End March 2004. **WEBSITE ESTABLISHED** Ongoing updating and modification as required.	KC to post new and updated information on Privacy website.
As Above	Implement on-line privacy training module developed by Privacy NSW and Dept of	Privacy Officer.	Adequate knowledge and information about privacy.	End 2003. **ON-LINE TRAINING UP ON WEB**	Kristin to complete training module.

	Commerce for NSW Govt agencies.			Ongoing review.	
As Above	Establish database/spreadsheet for recording issues, complaints and advice given related to privacy.	Privacy Officer.	Adequate knowledge and training about processes. Complaints officer appointed for UWS.	End June 2004. **Extended to End 2004.** Ongoing implementation and review.	KC to develop SS/DB for recording privacy queries and answers as they arise for future reference/posting on website.
As Above	Develop protocol for handling privacy enquiries and complaints.	UWS Complaints Officer. Privacy Officer. UWS Legal Counsel.	Adequate knowledge of complaints process and further external sources to refer to if required. Effective complaints handling.	End June 2004. **Extended to End 2004.** Complaints process being developed. Ongoing review.	Complaints process in development (Linda Watson – Complaints Officer). Privacy complaints will be integrated in to this process.
Functional Area:	**Academic Services Division**				
Issue for Consideration	**Proposed Strategy**	**Responsibility**	**Outcome/Comments**	**Completion/Review Date**	**Action**
Privacy considerations in teaching and learning.	Conduct review of privacy practices in teaching and learning context including: WebCT and on-line learning protocols and moderation/surveillance. Teacher/student privacy and confidentiality of information practices relating to potential dissemination or release of student personal information by lecturers. Student evaluations of teaching and units. Develop training and	Director Educational Development. Academic Registrar (or nominee). PVC Academic (or nominee). Assoc Deans of Colleges.	Clear guidelines for academic staff and students about privacy issues and practices relevant to their day to day academic work and interactions.	End June 2004. **Extended to End 2004.** Ongoing.	Consider some common issues to be posted on to Privacy website.

	information material for academic staff and students.				
Privacy considerations in personal information about students held by the Office of the Dean of Students.	Review practices in area of student counselling, student scholarships, Golden Key etc.	Dean of Students.	Certification that practices adhere to privacy requirements.	End March 2004. **Extended to End 2004.**	
Privacy Considerations in IT systems.	Review of ITS policies and procedures regarding privacy. Ensure all video surveillance activity is properly signposted and that there are proper procedures associated with the storage and use of surveillance tapes. Ensure Information Security Policy and practices protect personal data. Consider issue of mobile telephones with cameras.	Director ITS for all. Director Capital Works & Facilities. Security.	Certification that systems meet privacy requirements.	End June 2004. **Extended to End 2004.**	Email policy developed and awaiting approval. PW to review. Schedule for Oct/Nov.
Review of privacy in student administrative systems.	Review Callista system and protocols with respect to privacy requirements. Review student administration forms to ensure proper advise to students about privacy at UWS. Develop plain English brochure for students about privacy. Develop comprehensive	Academic Registrar (or nominee). Privacy Officer.	Certification that practices adhere to privacy requirements.	End September 2004. **Extended to End 2004.**	Callista review completed. Student forms review ongoing. Plain English brochure ongoing. Statement on release of student info ongoing. Training for staff organised and running.

	statement about procedures and requirements surrounding release of information about students. Develop training for ‘front line’ staff to ensure they have confidence in dealing with privacy.				

APPENDIX C – PRIVACY PRINCIPLES

Privacy and Personal Information Protection Act 1998 No 133 (EXTRACT)

Part 2 Information protection principles

Division 1 Principles

8 Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) A public sector agency must not collect personal information by any unlawful means.

9 Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

(a) the individual has authorised collection of the information from someone else, or

(b) in the case of information relating to a person who is under the age of 16 years—the information has been provided by a parent or guardian of the person.

10 Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

(a) the fact that the information is being collected,

(b) the purposes for which the information is being collected,

(c) the intended recipients of the information,

(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,

(e) the existence of any right of access to, and correction of, the information,

(f) the name and address of the agency that is collecting the information and the agency that is to hold the information.

11 Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete, and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

12 Retention and security of personal information

A public sector agency that holds personal information must ensure:

(a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

13 Information about personal information held by agencies

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the agency holds personal information, and

(b) whether the agency holds personal information relating to that person, and

(c) if the agency holds personal information relating to that person:

(i) the nature of that information, and

(ii) the main purposes for which the information is used, and

(iii) that person's entitlement to gain access to the information.

14 Access to personal information held by agencies

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

15 Alteration of personal information

(1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

(a) is accurate, and

(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

16 Agency must check accuracy of personal information before use

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

17 Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

(a) the individual to whom the information relates has consented to the use of the information for that other purpose, or

(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or

(c) the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

18 Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or

(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or

(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

19 Special restrictions on disclosure of personal information

(1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

(2) A public sector agency that holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales unless:

(a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or

(b) the disclosure is permitted under a privacy code of practice.

(3) For the purposes of subsection (2), a ***relevant privacy law*** means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.

(4) The Privacy Commissioner is, within the year following the commencement of this section, to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales.

(5) Subsection (2) does not apply:

(a) until after the first anniversary of the commencement of this section, or

(b) until a code referred to in subsection (4) is made, whichever is the later.

APPENDIX D

Health Records and Information Privacy Act 2002 No 71

Schedule 1 Health Privacy Principles

(Section 4)

1 Purposes of collection of health information

(1) An organisation must not collect health information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) An organisation must not collect health information by any unlawful means.

2 Information must be relevant, not excessive, accurate and not intrusive

An organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

3 Collection to be from individual concerned

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

4 Individual to be made aware of certain matters

(1) An organisation that collects health information about an individual from the individual must, at or before the time that it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following:

(a) the identity of the organisation and how to contact it,

(b) the fact that the individual is able to request access to the information,

(c) the purposes for which the information is collected,

(d) the persons to whom (or the types of persons to whom) the organisation usually discloses information of that kind,

(e) any law that requires the particular information to be collected,

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

(2) If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is generally aware of the matters listed in subclause (1) except to the extent that:

(a) making the individual aware of the matters would pose a serious threat to the life or health of any individual, or

(b) the collection is made in accordance with guidelines issued under subclause (3).

(3) The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).

(4) An organisation is not required to comply with a requirement of this clause if:

(a) the individual to whom the information relates has expressly consented to the organisation not complying with it, or

(b) the organisation is lawfully authorised or required not to comply with it, or

(c) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or

(e) the information concerned is collected for law enforcement purposes, or

(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

(5) If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause

(1), the organisation must take steps that are reasonable in the circumstances to ensure that any authorised representative of the individual is aware of those matters.

(6) Subclause (4) (e) does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

5 Retention and security

(1) An organisation that holds health information must ensure that:

(a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and

(c) the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of the organisation is done to prevent unauthorised use or disclosure of the information.

Note. Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

(2) An organisation is not required to comply with a requirement of this clause if:

(a) the organisation is lawfully authorised or required not to comply with it, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

(3) An investigative agency is not required to comply with subclause (1) (a).

6 Information about health information held by organisations

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable to enable any individual to ascertain:

(a) whether the organisation holds health information, and

(b) whether the organisation holds health information relating to that individual, and

(c) if the organisation holds health information relating to that individual:

(i) the nature of that information, and

(ii) the main purposes for which the information is used, and

(iii) that person's entitlement to request access to the information.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

7 Access to health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

Note. Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Access to health information held by public sector agencies may also be available under the *Freedom of Information Act 1989* or the *State Records Act 1998*.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

8 Amendment of health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information:

(a) is accurate, and

(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the individual to whom the information relates, the organisation must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.

Note. Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Amendment of health information held by public sector agencies may also be able to be sought under the *Freedom of Information Act 1989*.

(4) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

9 Accuracy

An organisation that holds health information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

10 Limits on use of health information

(1) An organisation that holds health information must not use the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless:

(a) **Consent**
the individual to whom the information relates has consented to the use of the information for that secondary purpose, or

(b) **Direct relation**
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or

> **Note.** For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare**
the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(d) **Management of health services**
the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training**
the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**
the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Find missing person**
the use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(h) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**
the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a health registration Act, or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(i) **Law enforcement**
the use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(j) **Investigative agencies**
the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(k) **Prescribed circumstances**
the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

11 Limits on disclosure of health information

(1) An organisation that holds health information must not disclose the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless:

(a) **Consent**
the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or

(b) **Direct relation**
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or

> **Note.** For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare**
the disclosure of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(d) **Management of health services**
the disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training**
the disclosure of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify the individual, the information is not made publicly available, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**
the disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Compassionate reasons**
the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:

(i) the disclosure is limited to the extent reasonable for those compassionate reasons, and

(ii) the individual is incapable of giving consent to the disclosure of the information, and

(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and

(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information, or

(h) **Find missing person**
the disclosure of the information for the secondary purpose is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(i) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**
the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a health registration Act, or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) **Law enforcement**
the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(k) **Investigative agencies**
the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(l) **Prescribed circumstances**
the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(c) the organisation is an investigative agency disclosing information to another investigative agency.

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) If health information is disclosed in accordance with subclause (1), the person, body or organisation to whom it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(6) The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

12 Identifiers

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the individual has consented to the adoption of the same identifier, or

(b) the use or disclosure of the identifier is required or authorised by or under law.

(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)–(k) or 11 (1) (c)–(l), or

(b) the individual has consented to the use or disclosure, or

(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or

(b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

13 Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

14 Transborder data flows and data flow to Commonwealth agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or

(b) the individual consents to the transfer, or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual,

(ii) it is impracticable to obtain the consent of the individual to that transfer,

(iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or

(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

15 Linkage of health records

(1) An organisation must not:

(a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or

(b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(c) the inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

(3) In this clause:

health record means an ongoing record of health care for an individual.

health records linkage system means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

APPENDIX E – INTERNAL REVIEW APPLICATION FORM

Privacy Complaint: Internal Review Application Form
University of Western Sydney

This is an application[i] for review of conduct under section 53 of the Privacy and Personal Information Protection Act 1998 (PPIPA). Refer also to the University's Privacy Management Plan and Policy (http://www.uws.edu.au/privacy)

1.	Name of agency[ii] you are complaining about: UNIVERSITY OF WESTERN SYDNEY
2.	Your full name:
3.	Your postal address or indicate the address to which you wish correspondence to be directed:
4.	If you are complaining on behalf of someone else, write their full name here: What is your relationship to this other person (eg. parent)? Is the other person capable of making the complaint him or herself? ❑ **Yes** ❑ **No** ❑ **I'm not sure**
5.	What is the specific ***conduct***[iii] you are complaining about?
6.	Please tick which of the following describes your complaint: *(You can tick more than one)* ❑ collection of my personal information ❑ security or storage of my personal information ❑ refusal to let me access or find out about my own personal information ❑ accuracy of my personal information ❑ use of my personal information

	❑ disclosure of my personal information ❑ other ❑ I'm not sure
7.	When did the conduct occur? *(Please be as specific as you can)*
8.	When did you first become aware of this conduct?
9.	You need to lodge this application within 6 months of the date you have written at Q.8. If more than 6 months has passed, you need to ask the agency for special permission to lodge a late application. If you need to, write here to explain why you have taken more than 6 months to make your complaint:
10	What effect did the conduct have on you?
11	What effect might the conduct have on you in the future?
12	What would you like to see the agency do about the conduct? *(For example : an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)*
13	I understand that this form will be used by the University to process my request for an Internal Review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with section 54 (1) of the Privacy and Personal Information Protection Act 1998 and that the Privacy Commissioner will be kept advised of the progress of the review.
14	I would prefer the Privacy Commissioner to have: ❑ a copy of this application form, or ❑ just the information provided at Q's 5 - 12.

Your signature:

Dated:

NOW SEND THE COMPLETED FORM TO:
Rhonda Hawkins, University Secretary
Division of Corporate Services
University of Western Sydney
Frogmore House, Building AA
PO Box 1000, ST MARYS NSW 2760

Or you can email the form to: privacy@uws.edu.au

Keep a copy for your own records

APPENDIX F – INTERNAL REVIEW GUIDELINES FOR STAFF

PRIVACY COMPLAINT / INTERNAL REVIEW
CHECKLIST FOR THE RESPONDENT AGENCY

This checklist helps NSW public sector agencies carry out Internal Reviews of conduct under section 53 of the Privacy and Personal Information Protection Act 1998

	Steps to follow	**Date completed**
	Preliminary steps	
1	Is the complaint about the complainant's *personal information* (or the personal information of the person they are representing)?[iv] ❑ Yes – You should treat their complaint as a request for Internal Review under the PPIP Act. Go to Q.2. ❑ No – Follow your agency's normal complaint handling procedures.	
2	According to the complainant, when did the alleged conduct occur?	
3	Is the complaint about conduct that occurred since 1 July 2000? ❑ Yes – Go to Q.4. ❑ No – The PPIP Act does not apply. Follow your agency's normal complaint handling procedures.	
4	According to the complainant, when did they first *become aware of* the alleged conduct?[v]	
	When was this application / privacy complaint first lodged?[vi]	
6	If more than six months lapsed between the date at Q.4 and the date at Q.5, your agency must decide whether you will accept a late application.[vii] Will you accept this late application? ❑ Yes – Go to Q.7. ❑ No – Explain your reasons to the complainant, then follow your agency's normal complaint handling procedures.	
7	When will 60 days elapse from the date at Q.5? After this date the complainant may go to the Administrative Decisions Tribunal without waiting for the results of this review.	

8	Tick all of the following types of ***conduct***[viii] which describe the complaint: ❑ collection of the complainant's personal information (IPPs 1-4) ❑ security or storage of the complainant's personal information (IPP 5) ❑ refusal to let the complainant access or find out about their own personal information (IPPs 6-7) ❑ accuracy or relevance of the complainant's personal information (IPPs 8-9) ❑ use of the complainant's personal information (IPP 10) ❑ disclosure of the complainant's personal information (IPPs 11-12, and/or the public register provisions in Part 6 of the Act) ❑ other / it's not clear	
9	Appoint a reviewing officer. *(The reviewing officer must be someone who was not substantially involved in any matter relating to the conduct complained about. For other requirements see s.53(4) of the PPIP Act.)* Insert the reviewing officer's name here:	
10	Write to the complainant, stating: ❑ your understanding of the conduct complained about ❑ your understanding of the privacy principle/s at issue (see Q.8) ❑ that the agency is conducting an Internal Review under the PPIP Act ❑ the name, title, and contact details of the reviewing officer ❑ how the reviewing officer is independent of the person/s responsible for the alleged conduct ❑ the estimated completion date for the review process ❑ that if your review is not complete by the date at Q.7, the complainant can go to the ADT for an external review of the alleged conduct ❑ that a copy of this letter will be provided to the NSW Privacy Commissioner for their oversight role	
11	Send a copy of your letter at Q.10 to the NSW Privacy Commissioner, at PO Box A2122, Sydney South, NSW 1235; or fax (02) 9268 5501. If the complainant has consented[ix], include a copy of the complainant's application – either the whole application or just the information provided at Q's 5-12 on the *Privacy Complaint : Internal Review Application Form*.	
	Conducting the review itself	
12	Start the review. You need to determine: ❑ whether the alleged conduct occurred, ❑ if so, whether the conduct complied with all the IPPs (and the Part 6 public register provisions, if applicable)[x], and ❑ if the conduct did not comply with an IPP (or the public register provisions), whether the non-compliance was authorised by: o an exemption under the PPIP Act[xi], o a Privacy Code of Practice[xii], or o a s.41 Direction from the Privacy Commissioner[xiii].	

13	Four weeks after sending the letter at Q.10, send a progress report to the complainant and the Privacy Commissioner[xiv]. Include: ❑ an explanation of any reasons for delay ❑ a revised estimated completion date for the review process ❑ a reminder that if the review is not complete by the date at Q.7, the complainant can go to the ADT for an external review of the alleged conduct	
	On completion of the review	
14	Write up your findings about the facts, the law, and your interpretation of the law. Set out your preliminary determination about: ❑ whether there was sufficient evidence to establish that the alleged conduct occurred ❑ which of the IPPs (and/or the public register provisions) you examined and why ❑ whether the conduct complied with the IPPs / public register provisions ❑ if the conduct did not comply with an IPP (or public register provisions), whether the non-compliance was authorised by: o an exemption under the PPIP Act, o a Privacy Code of Practice, or o a s.41 Direction from the Privacy Commissioner. ❑ an appropriate action for the agency by way of response/remedy.	
15	Before completing the review, check whether the Privacy Commissioner wishes to make a submission. Ideally you should provide a draft copy of your preliminary determination to the Privacy Commissioner for comment.	
16	Finalise your determination of the Internal Review, by making one of the following **findings**: ❑ insufficient evidence to suggest alleged conduct occurred ❑ alleged conduct occurred but complied with the IPPs / public register provisions ❑ alleged conduct occurred; did not comply with the IPPs /public register provisions; but non-compliance was authorised by an exemption, Code or s.41 Direction ❑ alleged conduct occurred; the conduct did not comply with the IPPs / public register provisions; the non-compliance was not authorised **("a breach")**	
17	Did the agency breach an IPP or the public register provisions? ❑ **Yes** – go to Q. 19 ❑ **No** – go to Q. 18	
18	Even though the agency did not breach any IPP or the public register provisions, have you identified any need for improvement in policies, procedures, communication with your clients, etc? ❑ Yes – go to Q. 19 ❑ No – go to Q.21	
19	What action is proposed by the agency as a result of this review? *(You can have more than one)* ❑ apology to complainant ❑ rectification[xv] to complainant, eg: o access to their personal information o correction of their personal information o other type of rectification ❑ expenses to be paid to complainant	

	❑ compensatory damages paid to complainant ❑ other remedy to complainant ❑ review of policies, practices or systems ❑ change in policies, practices or systems ❑ training (or further training) for staff ❑ other action ❑ no action	
20	Is the proposed action likely to match the expectations of the complainant? ❑ **Yes** ❑ **No** ❑ **Unsure**	
21	Notify the complainant and the Privacy Commissioner[xiv] in writing: ❑ that you have completed the Internal Review ❑ what your **findings** are, ie. which one of the following: o insufficient evidence to suggest alleged conduct occurred o alleged conduct occurred but complied with the IPPs / public register provisions o alleged conduct occurred; did not comply with the IPPs / public register provisions; but non-compliance authorised by an exemption, Code or s.41 Direction o alleged conduct occurred; the conduct did not comply with the IPPs / public register provisions; the non-compliance was not authorised **("a breach")** ❑ what the **reasons** for your findings are ❑ a plain English explanation of the **law** behind your findings, including quoting in full the relevant legislative provisions you are talking about ❑ what action/s you are going to take as a result ❑ that the complainant has the right to apply the Administrative Decisions Tribunal (within 28 days of the date of the decision) for a review of the conduct complained about ❑ the contact details for the ADT	
22	Keep a record of this review for your annual reporting requirements[xvii]	

ENDNOTES: More information for public sector agencies

[i] It is not a requirement under the PPIP Act that you complete an application form. This form is designed for your convenience only. It was developed by Privacy NSW and has been adapted for use in UWS.

[ii] The PPIP Act regulates NSW State government departments, Area Health Services, most other State government bodies, NSW local councils and universities. Each of these is defined as a "public sector agency".

[iii] 'Conduct' can include an action, a decision, or even inaction by the agency. For example the 'conduct' in your case might be a *decision* to refuse you access to your personal information, or the *action* of disclosing your personal information to another person, or the *inaction* of a failure to protect your personal information from being inappropriately accessed by someone else.

[iv] "Personal information" is defined at s.4 of the PPIP Act as "information or an opinion … about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion". There are some exemptions to the definition (eg. for "information or an opinion about an individual's suitability for appointment or employment as a public sector official") so check s.4 in full. However if you are thinking of relying on one of these exemptions, especially s.4(3)(b) or s.4(3)(j), please first seek advice from Privacy NSW as to the extent to which the exemption applies.

[v] Note that in *Y v DET*, the ADT warned against agencies using 'self-serving calculations' when determining the date on which the complainant may have first become aware of the conduct complained of.

[vi] In *Y v DET*, the ADT found that "express reference" to the PPIP Act is not essential in correspondence with agencies, especially where the context suggests that a statutory right is being invoked. Therefore the complainant need not have used the phrase 'Internal Review' for their privacy complaint to be considered by law to be an Internal Review application. Agencies should therefore look to the date the first written complaint about a breach of privacy was made.

[vii] Your agency should have a clear and written policy on the grounds under which you will allow a late application, including the means by which you will notify complainants about those grounds and what the complainant must prove to you. Include your policy in your Privacy Management Plan. For more on this issue see the April 2003 *PCO Newsletter*, available on our website via http://www.lawlink.nsw.gov.au/pc.nsf/pages/generalinfo

[viii] 'Conduct' can include an action, a decision, or even inaction by your agency. For example the 'conduct' in this case might be a *decision* to refuse the complainant access to his or her personal information, or the *action* of disclosing his or her personal information to another person, or the *inaction* of a failure to protect the complainant's personal information from being inappropriately accessed by someone else.

[ix] See Q.14 on the *Privacy Complaint : Internal Review Application Form*, if they have used that form. (It is not compulsory for the complainant to use any particular format, so long as their request is in writing.)

[x] Don't forget to look at all the IPPs, as they can be inter-related. For example a complaint about disclosure (IPPs 11 and 12 and the public register provisions) might also raise issues about data security under IPP 5, or notification about collection at IPP 3.

[xi] Exemptions are found in the PPIP Act at sections 6, 20, and 23-28.

[xii] Privacy Codes of Practice are instruments made by the Attorney General. Many can be found on the Privacy NSW website at:
http://www.lawlink.nsw.gov.au/pc.nsf/pages/codesmade

[xiii] Section 41 Directions only modify the IPPs, not the public register provisions. They are usually temporary so check the dates carefully, and contact Privacy NSW for earlier versions of Directions if necessary. All current s.41 Directions can be found at:
http://www.lawlink.nsw.gov.au/pc.nsf/pages/section41orders

[xiv] You are obliged under s.54(1)(b) to keep the Privacy Commissioner notified of progress.